

| | |
|---|--|
| Integrated Public Safety Commission Project Hoosier SAFE-T | System Policy Manual Section I (b) Zone Database Management |
|---|--|

Zone Database Management

Section I (b)

Policies

- (a) The Integrated Public Safety Commission staff is responsible for managing and maintaining Project Hoosier SAFE-T system wide databases. The designated System Administrator has responsibility for administration of all fleetmapping related activities, i.e., maintain the security of the system keys, issuance and maintenance of subscriber and talkgroup ID's.
- (b) The System Administrator will ensure that system wide databases are routinely backed up, and that relevant information technology "best practices" are implemented.

1) Background

The purpose of this policy is to establish responsibilities for managing and maintaining system wide infrastructure and subscriber/user databases. These databases contain objects for the system & sub-systems, which define the operational characteristics (personality) of the following:

- Subscriber Radios.
- Radio Users.
- Talkgroups & Multigroups.
- Profiles for Radio Users & Talkgroups.
- Fleetmap programming at the system level.
- System & Subsystem equipment operational parameters.
- Security Groups.

- Login User accounts & privileges.

System databases, referred to in this section, do not contain equipment-programming parameters for the local and wide area networking hardware such as routers, switches, hubs, and channel banks. Nor does the database contain the software load information for servers & client computers.

2) Capabilities

Each Smart Zone Master Site houses several central subscriber databases; however, the management of the database can be performed by the user agencies staff responsible for the various aspects of the data in the database. For example, local agencies who have purchased Zone Manager Workstations may perform database updates/changes to those subscribers contained in their respective security group. However there is a 32-site limitation per zone.

System wide databases contain the operational personality of the entire system. Due to the critical nature of this data environment, system wide databases must be routinely backed up every two weeks.

Operational Context:

- a) System databases are partitioned to facilitate the distributed management of the data contained in the database. Each agency system manager shall manage the portions of the above listed data for which they have responsibility. System Managers may request the Project Hoosier SAFE-T staff to assist with the management of their data.
- b) Individual agencies responsible for maintaining & archiving their own security group files as defined by the agencies internal procedures.
- c) Multiple database backups will be made. Media will be maintained at the site of origin, an additional copy will be forwarded to the Project Hoosier SAFE-T System Administrator, with a third copy to be stored at an “off-site” facility. Database restores will be performed under the direction of the System Administrator, typically, in the event of an operating system or version upgrade, database corruption or failure. Multiple revisions of backups will be dated and kept in a rotating

| | |
|---|--|
| Integrated Public Safety Commission Project Hoosier SAFE-T | System Policy Manual Section I (b) Zone Database Management |
|---|--|

stock, so that a restore would be possible from an earlier backup if the need arises. The following database backups labeling convention shall be used:

Zone #_Database Name_Date (01012004) Tape 1,2, etc.
Example - Zone 1_UCS_01012004 1

The Project Hoosier System Administrator shall notify agency system managers of any database issues that may adversely impact those entities.

Recommendations:

- a) This will be an ongoing task in the operation & management of the system.

Procedure:

- a) The methods for performing the database operations are defined in relative technical resource manuals and training for the system.

Management

- a) Agency Systems Managers are responsible for managing the various user/subscriber databases over which they have responsibility.